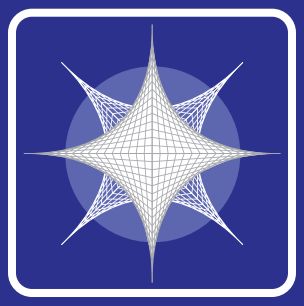


FORTINET

Fortinet Security Fabric Upgrade Guide

VERSION 6.0.4

FORTIOS VERSION 6.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

January 11, 2019

Fortinet Security Fabric Upgrade Guide

01-604-513725-20190111

TABLE OF CONTENTS

Change log

Date	Change description
January 11, 2019	Initial release.

Introduction

This guide describes how to upgrade the Fortinet devices in your network when you have two or more different devices that belong to a Fortinet Security Fabric. By using this guide, you make sure that devices are upgraded in the proper order, using compatible firmware versions.

Because the upgrading procedure can disrupt your network traffic, it's recommended that you perform upgrades to the Security Fabric devices during a maintenance window.

Before upgrading a device, review the release notes for the new firmware version. Release notes are available in the Fortinet Documentation Library.

For information about firmware compatibility, see the Fortinet Security Fabric Compatibility Matrix - FortiOS and Fortinet Security Fabric Compatibility Matrix - FortiSandbox.

Upgrading the Fortinet Security Fabric

This section describes how to upgrade the devices that you use in your Security Fabric in the correct order when you upgrade from FortiOS 5.6.1 and later to FortiOS 6.0.4.

Upgrade order

When you upgrade your Security Fabric, it's recommended that you follow the order listed below so that devices that manage other devices are upgraded first. Not all products listed are required by a Security Fabric. If you don't use a product in your network or don't need to upgrade it, skip to the next product in the list.

If you're upgrading both FortiOS and FortiClient from 5.6 to 6.0, you should upgrade FortiClient first to avoid compatibility issues.

The upgrade order is as follows:

1. Upgrade FortiAnalyzer
2. Upgrade FortiManager
3. Upgrade FortiGate devices
4. Upgrade managed FortiSwitch devices
5. Upgrade managed FortiAP devices
6. Upgrade FortiClient EMS
7. Upgrade FortiClient
8. Upgrade FortiSandbox
9. Upgrade FortiMail

Upgrade FortiAnalyzer

FortiOS 6.0.4 supports FortiAnalyzer 6.0.4.

1. Go to the Fortinet Support website and download the FortiAnalyzer firmware.
2. In FortiAnalyzer, go to **System Settings > Dashboard**. In the **System Information** widget, go to the **System Configuration** field, and select the **Backup** icon. Save the backup of your current FortiAnalyzer configuration, in case you need to restore it after the upgrade process.
3. In the **System Information** widget, go to the **Firmware Version** field, and select the **Upgrade Firmware** icon.
4. In the **Firmware Upload** dialog box, select **Browse** and locate the firmware. Select **Open** and select **OK**.
5. After the FortiAnalyzer uploads the firmware and reboots, go to **System Settings > Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware Version**.

For more information, see the FortiAnalyzer Release Notes and FortiAnalyzer Administration Guide.

Upgrade FortiManager

FortiOS 6.0.4 supports FortiManager 6.0.4.

1. Go to the Fortinet Support website, and download the FortiManager firmware.
2. In FortiManager, go to **System Settings > Advanced > Advanced Settings**, and enable **Offline Mode** to stop automatic updates during the upgrade.
3. Go to **System Settings > Dashboard**. In the **System Information** widget, go to the **System Configuration** field, and select the **Backup** icon. Save the backup of your current FortiManager configuration, in case you need to restore it after the upgrade process.
4. In the **System Information** widget, go to the **Firmware Version** field, and select the **Upgrade Firmware** icon.
5. In the **Firmware Upload** dialog box, select **Browse** and locate the firmware. Select **Open** and select **OK**.
6. After the FortiManager uploads the firmware and reboots, go to **System Settings > Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware Version**.
7. In **System Settings > Advanced > Advanced Settings**, disable **Offline Mode**.

For more information, see the FortiManager Release Notes and FortiManager Administration Guide.

Upgrade FortiGate devices

All FortiGate devices in the Security Fabric must use the same firmware version. Upgrade the root FortiGate before upgrading the other FortiGate devices.

You must upgrade FortiAnalyzer to 6.0.4 before upgrading any FortiGate devices to 6.0.4.

1. Go to **System > Firmware**. The new firmware is shown.
2. Under **FortiGuard Firmware**, select **Latest**. You can also download firmware from the Fortinet Support website and then upload it manually to your FortiGate.

A notice may appear stating that there is no valid upgrade path for this firmware version. In this case, select **All available** instead and find a suitable firmware version for your FortiGate.

For more information about the upgrade path, use the Upgrade Path Tool.

3. Select **Backup config and upgrade**. When prompted, select **Continue**.
4. Save the backup of your current FortiGate configuration, in case you need to restore it after the upgrade process.
5. After the FortiGate uploads the firmware and reboots, go to the **Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware**.

For more information, see the FortiOS Release Notes and FortiOS Handbook.

Upgrade managed FortiSwitch devices

FortiOS 6.0.4 supports FortiSwitch 3.6.4 and later.

1. Connect to the FortiGate that manages the FortiSwitch.
2. Go to **WiFi & Switch Controller > Managed FortiSwitch**. Select the FortiSwitch and select **Edit**. If new firmware is available, a message from FortiGuard appears. Select **Upgrade**. You can also upload the firmware manually from your computer.
3. After the FortiSwitch uploads the firmware and reboots, go to **WiFi & Switch Controller > Managed FortiSwitch**, select the FortiSwitch, and select **Edit**. Confirm that **Firmware** displays the correct version.

After upgrading, you must manually create a firewall policy to allow RADIUS traffic for 802.1x authentication from the FortiSwitch (for example, from the FortiLink interface) to the RADIUS server through the FortiGate.

For more information, see the FortiSwitch Release Notes and Managed Switch Administration Guide.

Upgrade managed FortiAP devices

FortiOS 6.0.4 supports FortiAP 5.4.2 and later. However, it's recommended that you upgrade to FortiAP 5.6.0 and later to access all of the new features.

FortiOS 6.0.4 supports FortiAP-S 5.4.3 and later. However, it's recommended that you upgrade to FortiAP-S 5.6.0 and later to access all of the new features.

1. Connect to the FortiGate that manages the FortiAP.
2. Go to **WiFi & Switch Controller > Managed FortiAPs** and make sure the device **State** is **Online**.
3. Select the FortiAP and select **Edit**. If new firmware is available, a message from FortiGuard appears. Select **Upgrade**. You can also upload the firmware manually from your computer.
4. After the FortiAP uploads the firmware and reboots, go to **WiFi & Switch Controller > Managed FortiAPs**. Confirm that **OS Version** displays the correct firmware.

For more information, see the FortiAP Release Notes and FortiAP Configuration Guide.

Upgrade FortiClient EMS

FortiOS 6.0.4 supports FortiClient EMS 6.0.0 and later.

To ensure a successful upgrade, it's recommended that you perform the upgrade on a staging server before upgrading the production server.

1. Connect FortiClient endpoints to the staging server.
2. Connect to the staging server. A notification appears about the new firmware. Review and accept the upgrade. You can also download the installer for the new firmware by going to the Fortinet Support website and manually running the installer.

For information about the FortiClient EMS upgrade path, see the Fortinet Documentation Library.

3. After the installation, go to **Dashboard > FortiClient Status**. Confirm that the **System Information** widget displays the correct firmware.
4. Monitor the staging server for two days. If there are no issues, upgrade the production server to the new firmware and reconnect FortiClient endpoints to the production server.

For more information, see the FortiClient EMS Release Notes and FortiClient EMS Administration Guide.

Upgrade FortiClient

For Microsoft Windows, macOS, and Linux, FortiOS 6.0.4 supports FortiClient 6.0.0 and later.

For iOS, FortiOS 6.0.4 supports 5.6.0 and later.

For Android, FortiOS 6.0.4 supports 5.4.2 and later.

You can either upgrade FortiClient manually on each device or you can use FortiClient EMS to push the upgrade to all devices.

Manual upgrade

1. Open FortiClient and go to **About**.
2. Beside the number of your current version, select **Update Available**. You can also download the latest version from the FortiClient website.

For information about the FortiClient upgrade path, see the Fortinet Documentation Library.

3. After the upgrade process is complete, go to **About** to confirm that you're using the right version.

For more information, see the FortiClient Release Notes and FortiClient Administration Guide.

FortiClient EMS upgrade

1. Connect to FortiClient EMS and deploy the installer package for FortiClient.

For information about the FortiClient upgrade path, see the Fortinet Documentation Library.

2. A prompt appears on the FortiClient endpoint when an installer package is requested to be deployed. Users can select one of the following:
   - **Upgrade Now**: The upgrade is performed immediately and the endpoint reboots automatically.
   - **Upgrade Later**: A time is selected for the update to be performed (8 PM by default). The endpoint reboots automatically after the update is finished.
   - No option: If no option is selected, the upgrade occurs by default at 8 PM. After the upgrade occurs, a prompt appears asking the user to either reboot the endpoint immediately or reboot it later. It's recommended to perform the update immediately.
3. On FortiClient EMS, go to **Software Inventory > Applications** and make sure that the proper version of FortiClient appears.

For more information, see the FortiClient EMS Release Notes and FortiClient EMS Administration Guide.

Upgrade FortiSandbox

FortiOS 6.0.4 supports FortiSandbox 2.3.3 and later.

1. Go to the Fortinet Support website and download the FortiSandbox firmware.
2. Go to the **Dashboard.** In the **System Information** widget, go to the **Firmware Version** field, and select **Update**.
3. Select **Choose File** and locate the firmware.
4. Select **Submit** to start the upgrade.
5. After the FortiSandbox uploads the firmware and reboots, go to the **Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware Version**.

For more information, see the FortiSandbox Release Notes and FortiSandbox Administration Guide.

Upgrade FortiMail

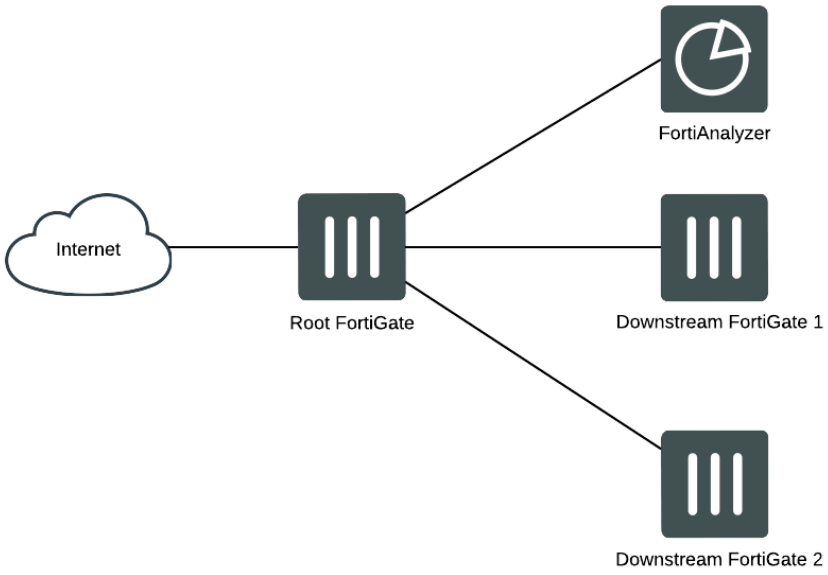
To use Security Fabric features, you must use FortiMail 6.0.0 or later.

1. Go to the Fortinet Support website and download the FortiMail firmware.
2. Go to the Dashboard. In the **System Information** widget, go to the **Firmware Version** field, and select **Update**.
3. Locate and select the firmware.
4. After the FortiMail uploads the firmware and reboots, go to the **Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware version**.

For more information, see the FortiMail Release Notes and FortiMail Administration Guide.

Case study: FortiGate and FortiAnalyzer

The following case study includes four devices in total: three FortiGate devices and a FortiAnalyzer.



In this example, you upgrade all four devices from 6.0.3 to 6.0.4 in the following order: the FortiAnalyzer, the root FortiGate, downstream FortiGate 1, and downstream FortiGate 2. You then run a Security Fabric Rating, to verify that all devices are operating as expected and that all FortiGate devices use the same firmware version.

Before upgrading, be sure to read all release notes, verify firmware compatibility using the Fortinet Security Fabric Compatibility Matrix - FortiOS and Fortinet Security Fabric Compatibility Matrix - FortiSandbox, and use the Upgrade Path Tool.

Upgrade the FortiAnalyzer

1. Go to the Fortinet Support website and download the FortiAnalyzer 6.0.4 firmware.
2. Connect to the FortiAnalyzer.
3. In FortiAnalyzer, go to **System Settings > Dashboard**. In the **System Information** widget, go to the **System Configuration** field, and select the **Backup** icon. Save the backup of your current FortiAnalyzer configuration, in case you need to restore it after the upgrade process.
4. In the **System Information** widget, go to the **Firmware Version** field, and select the **Upgrade Firmware** icon.
5. In the **Firmware Upload** dialog box, select **Browse** and locate the firmware. Select **Open** and select **OK**.
6. After the FortiAnalyzer uploads the firmware and reboots, go to **System Settings > Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware Version.**

Upgrade the root FortiGate

1. Connect to the root FortiGate.
2. Go to **System > Firmware**. The new firmware is shown.
3. Under **FortiGuard Firmware**, select **Latest**. You can also download firmware from the Fortinet Support website and then upload it manually to your FortiGate.
4. Select **Backup config and upgrade**. When prompted, select **Continue**.
5. Save the backup of your current FortiGate configuration, in case you need to restore it after the upgrade process.
6. After the FortiGate uploads the firmware and reboots, go to the **Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware**.

Upgrade downstream FortiGate 1

The two downstream FortiGate devices can be upgraded simultaneously.

1. Connect to downstream FortiGate 1.
2. Go to **System > Firmware**. The new firmware is shown.
3. Under **FortiGuard Firmware**, select **Latest**. You can also download firmware from the Fortinet Support website and then upload it manually to your FortiGate.
4. Select **Backup config and upgrade**. When prompted, select **Continue**.
5. Save the backup of your current FortiGate configuration, in case you need to restore it after the upgrade process.
6. After the FortiGate uploads the firmware and reboots, go to the **Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware**.

Upgrade downstream FortiGate 2

1. Connect to downstream FortiGate 2.
2. Go to **System > Firmware**. The new firmware is shown.
3. Under **FortiGuard Firmware**, select **Latest**. You can also download firmware from the Fortinet Support website and then upload it manually to your FortiGate.
4. Select **Backup config and upgrade**. When prompted, select **Continue**.
5. Save the backup of your current FortiGate configuration, in case you need to restore it after the upgrade process.
6. After the FortiGate uploads the firmware and reboots, go to the **Dashboard**. Confirm that the **System Information** widget displays the correct **Firmware**.

Run a Security Fabric Rating

1. Connect to the root FortiGate.
2. Go to **Security Fabric > Security Rating** and select **Run Now**.
3. After the check is complete, select **All Results**.
4. Verify that all FortiGate devices in the Security Fabric passed the following checks:
   - **FortiAnalyzer**:All FortiGate devices in the Security Fabric can connect to and authenticate with their configured FortiAnalyzer.
   - **Compatible Firmware**: All FortiGate devices in the Security Fabric should run the same firmware version.